IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: M. ARIMOTO, et al.

Application No.: New Patent Application

Filed: October 10, 2003

For: NETWORK MONITORING SYSTEM

CLAIM FOR PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

Sir:

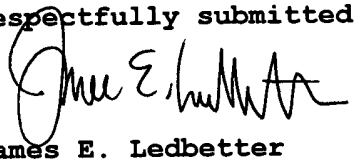
The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. 2002-299997, filed October 15, 2002.

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,



Date: October 10, 2003

James E. Ledbetter
Registration No. 28,732

JEL/apg
Attorney Docket No. L8612.03103
STEVENS, DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, NW, Suite 850
P.O. Box 34387
Washington, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月１５日

出願番号
Application Number: 特願２００２－２９９９９７

[ST. 10/C]: [ＪＰ２００２－２９９９９７]

出願人
Applicant(s): 株式会社山武

２００３年　８月１２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０６４６３９

【書類名】　特許願
【整理番号】　20020274
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号
　【氏名】　有元　伯治
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号
　【氏名】　関　英信
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号
　【氏名】　小森谷　良明
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号
　【氏名】　佐内　大司
【発明者】
　【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号
　【氏名】　三島　崇
【特許出願人】
　【識別番号】　000006666
　【氏名又は名称】　株式会社山武
【代理人】
　【識別番号】　100103894
　【弁理士】
　【氏名又は名称】　家入　健
【手数料の表示】
　【予納台帳番号】　106760
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0200107

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ネットワーク監視システム

【特許請求の範囲】

【請求項１】

一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークにおける通信状況を監視するネットワーク監視システムであって、

ネットワーク上を流れる複数のパケットを取得するデータ取得手段と、

前記データ取得手段により取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明情報を取得するデータ解析手段と、

前記データ解析手段によって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる表示情報を生成する表示情報生成手段とを備えたネットワーク監視システム。

【請求項２】

前記データ解析手段は、前記データ取得手段により取得された複数のパケットのそれぞれの種類を特定するステップと、種類の特定に応じて当該パケットよりアクション説明情報を取得するステップとを実行することを特徴とする請求項１記載のネットワーク監視システム。

【請求項３】

前記アクション説明情報には、送信元コンピュータ情報、宛先コンピュータ情報、アクション情報が含まれることを特徴とする請求項１記載のネットワーク監視システム。

【請求項４】

前記データ解析手段によって取得されたアクション説明情報を記憶する解析データ記憶手段をさらに備え、

前記表示情報生成手段は、ユーザの要求に応じて前記解析データ記憶手段に記憶されたアクション説明情報を再生表示させる表示情報を生成することを特徴とする請求項１記載のネットワーク監視システム。

【請求項５】

前記解析データ記憶手段に記憶されたアクション説明情報には、アクションの時刻に対応する時刻情報が含まれ、

前記表示情報生成手段は、ユーザの要求に応じて、アクションの時刻情報に従った再生表示を実行するための表示情報を生成することを特徴とする請求項４記載のネットワーク監視システム。

【請求項６】

前記表示情報生成手段は、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させることを特徴とする請求項４記載のネットワーク監視システム。

【請求項７】

前記表示情報生成手段は、ユーザによる表示の設定に従って表示情報を抽出し作成することを特徴とする請求項１記載のネットワーク監視システム。

【請求項８】

一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークにおける通信状況を監視するネットワーク監視方法であって、

ネットワーク上を流れる複数のパケットを取得するデータ取得ステップと、

前記データ取得ステップにより取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明情報を取得するデータ解析ステップと、

前記データ解析ステップによって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる表示情報を生成する表示情報生成ステップとを実行するネットワーク監視方法。

【請求項９】

前記データ解析ステップは、前記データ取得ステップにより取得された複数のパケットのそれぞれの種類を特定するステップと、種類の特定に応じて当該パケットよりアクション説明情報を取得するステップとを有することを特徴とする請求項８記載のネットワーク監視方法。

【請求項１０】

前記アクション説明情報には、送信元コンピュータ情報、宛先コンピュータ情

報及びアクション情報が含まれることを特徴とする請求項８記載のネットワーク監視方法。

【請求項１１】

前記データ解析ステップによって取得されたアクション説明情報を記憶する解析データ記憶ステップをさらに備え、

前記表示情報生成ステップは、ユーザの要求に応じて前記解析データ記憶ステップにより記憶されたアクション説明情報を再生表示させる表示情報を生成することを特徴とする請求項８記載のネットワーク監視方法。

【請求項１２】

前記解析データ記憶ステップにより記憶されたアクション説明情報には、アクションの時刻に対応する時刻情報が含まれ、

前記表示情報生成ステップは、ユーザの要求に応じて、アクションの時刻情報に従った再生表示を実行するための表示情報を生成することを特徴とする請求項１１記載のネットワーク監視方法。

【請求項１３】

前記表示情報生成ステップは、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させることを特徴とする請求項１１記載のネットワーク監視方法。

【請求項１４】

前記表示情報生成ステップは、ユーザによる表示の設定に従って表示情報を抽出し作成することを特徴とする請求項１記載のネットワーク監視方法。

【請求項１５】

一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークにおける通信状況を監視するネットワーク監視プログラムであって、このネットワーク監視プログラムは、コンピュータに対して

ネットワーク上を流れる複数のパケットを取得するデータ取得ステップと、

前記データ取得ステップにより取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明情報を取得するデータ解析ステップと、

前記データ解析ステップによって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる表示情報を生成する表示情報生成ステップとを実行させるネットワーク監視プログラム。

【請求項１６】

前記データ解析ステップは、前記データ取得ステップにより取得された複数のパケットのそれぞれの種類を特定するステップと、種類の特定に応じて当該パケットよりアクション説明情報を取得するステップとを有することを特徴とする請求項１５記載のネットワーク監視プログラム。

【請求項１７】

前記アクション説明情報には、送信元コンピュータ情報、宛先コンピュータ情報及びアクション情報が含まれることを特徴とする請求項１５記載のネットワーク監視プログラム。

【請求項１８】

前記データ解析ステップによって取得されたアクション説明情報を記憶する解析データ記憶ステップをさらに備え、

前記表示情報生成ステップは、ユーザの要求に応じて前記解析データ記憶ステップにより記憶されたアクション説明情報を再生表示させる表示情報を生成することを特徴とする請求項１５記載のネットワーク監視プログラム。

【請求項１９】

前記解析データ記憶ステップにより記憶されたアクション説明情報には、アクションの時刻に対応する時刻情報が含まれ、

前記表示情報生成ステップは、ユーザの要求に応じて、アクションの時刻情報に従った再生表示を実行するための表示情報を生成することを特徴とする請求項１８記載のネットワーク監視プログラム。

【請求項２０】

前記表示情報生成ステップは、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させることを特徴とする請求項１８記載のネットワーク監視プログラム。

【請求項２１】

前記表示情報生成ステップは、ユーザによる表示の設定に従って表示情報を抽出し作成することを特徴とする請求項１記載のネットワーク監視プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワーク上の通信状況を監視するためのネットワーク監視システム、ネットワーク監視方法及びネットワーク監視プログラムに関するものである。

【０００２】

【従来の技術】

近年、企業を中心に、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等のネットワークが構築され、広く普及している。一般にネットワークの運用では必ずトラブルが伴うことから、トラブルの予防と早期発見のためにネットワーク状態を監視するネットワーク・アナライザと呼ばれるネットワーク監視システムの導入が行われている。ネットワーク監視システムについては、例えば、下記特許文献１に開示されている。

【０００３】

他方、ネットワーク上に、例えばファイルサーバを設置し、データを複数のクライアントにおいて共有することが行われている。このファイルサーバ上のデータは、データの種類によっては、アクセスを制限し、消去・書き換えを制限する必要がある。このとき、ネットワーク監視システムにより、ネットワークを流れるデータパケットを監視し、どのクライアントがファイルサーバにアクセスしたかを確認することができる。

【０００４】

ここで、従来のネットワーク監視システムでは、パケット毎にそのパケットに含まれるデータの内容を解析し、画面に表示している。そのため、１パケット中に、アクションを説明するための情報、例えば、どのクライアントからどのクライアントのアクション対象に対してどのようなアクションが行われたかを示す情報が格納されている場合は、従来のネットワーク監視システムでも十分に通信状

況を把握することができる。しかしながら、例えば、マイクロソフト社が主に開発したＳＭＢ（Ｓｅｒｖｅｒ　Ｍｅｓｓａｇｅ　Ｂｌｏｃｋ）プロトコルでは、一アクションを説明するためのアクション説明情報が複数のパケットに分散され、送信されている。

【０００５】

ＳＭＢプロトコルにおけるパケットシーケンスの例を図１２に示す。この例では、クライアントがサーバの共有フォルダへ接続して、フォルダ内のファイルを書き換える操作を行った場合のパケットシーケンスの例を示す。図において、パケット番号は、個々のパケットに対して説明の便宜上割り振られた数字であり、１番から順にパケットが送受信されていることを示す。また、図における「Ｃ」はクライアントを示し、「Ｓ」はサーバを示す。このパケットシーケンスから、一アクションを説明するためのアクション説明情報が、３６個のパケットに分散されていることがわかる。

【０００６】

従って、このような一アクションを説明するためのアクション説明情報が複数のパケットに分散されるネットワークにおいて、従来のネットワーク監視システムにより一アクションを把握するためには、パケットに含まれるデータの内容の解析結果を、パケット毎に表示させた上で、ネットワーク監視者等のユーザが通信状況を分析しなければならない。そのため、多大な労力と知識を必要とすることになる。

【０００７】

【特許文献１】

特開２００２－６４４９２号公報

【０００８】

【発明が解決しようとする課題】

このように、従来のネットワーク監視システムでは、一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークを監視するためには、多大な労力と知識を必要とするという問題点があった。

【０００９】

本発明は、このような問題点を解決するためになされたもので、一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークを容易に監視することができるネットワーク監視システム、ネットワーク監視方法及びネットワーク監視プログラムを提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明にかかるネットワーク監視システムは、一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワーク（例えば本実施の形態におけるＳＭＢプロトコルに従ったネットワーク）における通信状況を監視するネットワーク監視システムであって、ネットワーク上を流れる複数のパケットを取得するデータ取得手段（例えば本実施の形態におけるデータ取得部３３２）と、前記データ取得手段により取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明情報を取得するデータ解析手段（例えば本実施の形態におけるデータ解析部３３）と、前記データ解析手段によって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる表示情報を生成する表示情報生成手段（例えば本実施の形態における表示情報生成部３４）とを備えたものである。このような構成により、ユーザは、一アクションを一画面上で認識することができるため、極めて容易に監視することができる。

【００１１】

ここで、データ解析手段は、前記データ取得手段により取得された複数のパケットのそれぞれの種類を特定するステップと、種類の特定に応じて当該パケットよりアクション説明情報を取得するステップとを実行するようにしてもよい。

【００１２】

好適な実施の形態におけるアクション説明情報には、送信元コンピュータ情報、宛先コンピュータ情報及びアクション情報が含まれる。

【００１３】

また、前記データ解析手段によって取得されたアクション説明情報を記憶する解析データ記憶手段をさらに備え、前記表示情報生成手段は、ユーザの要求に応

じて前記解析データ記憶手段に記憶されたアクション説明情報を再生表示させる表示情報を生成するようにしてもよい。これにより、ネットワーク上のアクションの確認作業をいつでも最適な時間に行うことができる。

【００１４】

ここで、前記解析データ記憶手段に記憶されたアクション説明情報には、アクションの時刻に対応する時刻情報が含まれ、前記表示情報生成手段は、ユーザの要求に応じて、アクションの時刻情報に従った再生表示を実行するための表示情報を生成するようにするとよい。これにより、時間的に実際の状況に従った再生表示を実現できる。

【００１５】

また、前記表示情報生成手段は、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させるようにしてもよい。これにより、再生表示による監視作業を効率化できる。また、前記表示情報生成手段は、ユーザによる表示の設定に従って表示情報を抽出し作成するようにしてもよい。

【００１６】

本発明にかかるネットワーク監視方法は、一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークにおける通信状況を監視するネットワーク監視方法であって、ネットワーク上を流れる複数のパケットを取得するデータ取得ステップと、前記データ取得ステップにより取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明情報を取得するデータ解析ステップと、前記データ解析ステップによって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる表示情報を生成する表示情報生成ステップとを実行するものである。このような方法により、ユーザは、一アクションを一画面上で認識することができるため、極めて容易に監視することができる。

【００１７】

ここで、前記データ解析ステップは、前記データ取得ステップにより取得された複数のパケットのそれぞれの種類を特定するステップと、種類の特定に応じて当該パケットよりアクション説明情報を取得するステップとを有するようにする

とよい。

【００１８】

好適な実施の形態におけるアクション説明情報には、送信元コンピュータ情報、宛先コンピュータ情報及びアクション情報が含まれる。

【００１９】

また、前記データ解析ステップによって取得されたアクション説明情報を記憶する解析データ記憶ステップをさらに備え、前記表示情報生成ステップは、ユーザの要求に応じて前記解析データ記憶ステップにより記憶されたアクション説明情報を再生表示させる表示情報を生成するようにするとよい。このような方法により、ネットワーク上のアクションの確認作業をいつでも最適な時間に行うことができる。

【００２０】

さらに、前記解析データ記憶ステップにより記憶されたアクション説明情報には、アクションの時刻に対応する時刻情報が含まれ、前記表示情報生成ステップは、ユーザの要求に応じて、アクションの時刻情報に従った再生表示を実行するための表示情報を生成するようにするとよい。これにより、時間的に実際の状況に従った再生表示を実現できる。

【００２１】

また、前記表示情報生成ステップは、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させることが望ましい。これにより、再生表示による監視作業を効率化できる。さらに、表示情報生成ステップは、ユーザによる表示の設定に従って表示情報を抽出し作成するようにしてもよい。

【００２２】

本発明におけるネットワーク監視プログラムは、一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークにおける通信状況を監視するネットワーク監視プログラムであって、このネットワーク監視プログラムは、コンピュータに対して、ネットワーク上を流れる複数のパケットを取得するデータ取得ステップと、前記データ取得ステップにより取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明

情報を取得するデータ解析ステップと、前記データ解析ステップによって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる表示情報を生成する表示情報生成ステップとを実行させるものである。このようなプログラムをコンピュータに実行させることにより、ユーザは、一アクションを一画面上で認識することができるため、極めて容易に監視することができる。

【００２３】

ここで、前記データ解析ステップは、前記データ取得ステップにより取得された複数のパケットのそれぞれの種類を特定するステップと、種類の特定に応じて当該パケットよりアクション説明情報を取得するステップとを有するとよい。

【００２４】

好適な実施の形態におけるアクション説明情報には、送信元コンピュータ情報、宛先コンピュータ情報及びアクション情報が含まれる。

【００２５】

また、前記データ解析ステップによって取得されたアクション説明情報を記憶する解析データ記憶ステップをさらに備え、前記表示情報生成ステップは、ユーザの要求に応じて前記解析データ記憶ステップにより記憶されたアクション説明情報を再生表示させる表示情報を生成するようにするとよい。このようなプログラムをコンピュータに実行させることにより、ネットワーク上のアクションの確認作業をいつでも最適な時間に行うことができる。

【００２６】

さらに、前記解析データ記憶ステップにより記憶されたアクション説明情報には、アクションの時刻に対応する時刻情報が含まれ、前記表示情報生成ステップは、ユーザの要求に応じて、アクションの時刻情報に従った再生表示を実行するための表示情報を生成するようにしてもよい。これにより、時間的に実際の状況に従った再生表示を実現できる。

【００２７】

前記表示情報生成ステップは、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させることが望ましい。これにより、再生表示による

監視作業を効率化できる。さらに、表示情報生成ステップは、ユーザによる表示の設定に従って表示情報を抽出し作成するようにしてもよい。

【００２８】

【発明の実施の形態】

最初に、本発明にかかるネットワーク監視システムが適用されるネットワーク構成について説明する。図１は、当該ネットワーク構成を示す構成図である。

【００２９】

図１に示されるように、このネットワーク構成は、複数のクライアントコンピュータ１、サーバ２、ネットワーク監視コンピュータ３、ＬＡＮ４、リピータハブ５を備えている。クライアントコンピュータ１とサーバ２及びクライアントコンピュータ１とネットワーク監視コンピュータ３は、ＬＡＮ４、リピータハブ５を介して通信可能に接続されている。

【００３０】

複数のクライアントコンピュータ１は、例えば、パーソナルコンピュータ（ＰＣ）や携帯端末であり、ＣＰＵ（中央制御装置）、ＲＯＭ、ＲＡＭ、ハードディスク、表示装置、入力装置、通信制御装置等のハードウェア構成を有する。

【００３１】

サーバ２は、例えば、ファイルサーバ、プリンタサーバ等の各種サーバであり、サーバコンピュータやＰＣにより構成される。以下の説明では、このサーバ２がファイルサーバの場合につき説明する。サーバ２は、ＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスク、表示装置、入力装置、通信制御装置等のハードウェア構成を有する。尚、サーバ２は、１台である必要はなく、複数台あってもよい。以下の例では、１台の例で説明する。

【００３２】

ネットワーク監視コンピュータ３は、ネットワーク監視システムを構成するものであり、例えば、パーソナルコンピュータ（ＰＣ）であり、ＣＰＵ、ＲＯＭ、ＲＡＭ、ハードディスク、表示装置、入力装置、通信制御装置等のハードウェア構成を有する。このネットワーク監視コンピュータ３は、ＬＡＮアナライザとも呼ばれる。本発明にかかるネットワーク監視コンピュータ３は、アプリケーショ

ンプログラムであるネットワーク監視プログラムがインストールされている。このネットワーク監視コンピュータ３は、ネットワーク上の通信状態を監視し、表示する機能を有する。尚、ネットワーク監視コンピュータ３は、小型ディスプレイと一体化された専用の携帯端末であってもよい。詳細な構成・動作については、後に詳述する。

【００３３】

ＬＡＮ４は、ネットワーク上の通信媒体として機能するものであり、この例では、通信プロトコルにＳＭＢプロトコルが採用されている。このＳＭＢプロトコルでは、上述のように、一アクションを説明するためのアクション説明情報が複数のパケットに分散して送信されている。

【００３４】

リピータハブ５は、サーバ２、ネットワーク監視コンピュータ３が並列に接続されている。そのため、サーバ２の送受信データは、ネットワーク監視コンピュータ３に対して送受信されるため、ネットワーク監視コンピュータ３は、サーバ２の送受信データを監視することができる。

【００３５】

続いて、図２を用いて、ネットワーク監視コンピュータ３の構成について説明する。図２に示されるように、このネットワーク監視コンピュータ３は、通信制御部３１、データ取得部３２、データ解析部３３、表示情報生成部３４、入出力制御部３５、取得データ記憶部３６、解析データ記憶部３７、表示装置３８及び入力装置３９を備えている。尚、本発明にかかるネットワーク監視コンピュータ３は、これら以外の機能ブロックをさらに備えていてもよい。

【００３６】

通信制御部３１は、ネットワーク上の他のコンピュータとの通信を制御するものであるが、本発明においては、特に、クライアント１とサーバ２間において送受信されるパケットと同様のパケットを受信する処理を制御する。

【００３７】

データ取得部３２は、クライアント１とサーバ２間において送受信されるパケットと同様のパケットからなるデータを取得する機能を有する。データ取得部３

２により取得されたデータは、取得データ記憶部３６に格納される。

【００３８】

データ解析部３３は、データ取得部３２によって取得されたパケットデータの解析を実行する機能を有する。本発明におけるデータ解析部３３は、特に、複数のパケットの種類を特定し、複数のパケットよりアクション説明情報を取得する機能を有する。データ解析部３３による解析の結果得られたデータは、解析データ記憶部３７に格納される。

【００３９】

表示情報生成部３４は、データ解析部３３によるデータ解析によって得られたアクション説明情報を表示装置３８に表示する表示情報を生成する機能を有する。

【００４０】

入出力制御部３５は、表示装置３８、入力装置３９の制御を実行する。この表示情報生成部３４は、後に詳述するプレイバック機能を有する。

【００４１】

取得データ記憶部３６は、データ取得部３２によって取得されたデータを一時的に格納するものであり、例えば、ハードディスク等の記憶手段により構成される。この取得データ記憶部３６は、例えば、一定の容量を持つサイクリックバッファによる構成される。例えば、１００メガバイト程度の記憶容量を有し、パケットを順次格納していき、全領域にデータが格納された状態になると、時間的に最も古いデータに上書きしていく。

【００４２】

解析データ記憶部３７は、データ解析部３３による解析の結果得られたデータを格納するものであり、例えば、ハードディスク等の記憶手段により構成される。

【００４３】

この解析データ記憶部３７に格納されたデータの例を図３に示す。図３に示されるように、解析データ記憶部３７には、送信元コンピュータ情報、宛先コンピュータ情報、ユーザ情報、アクション対象情報、アクション情報及び時刻情報が

相互に関連付けられて格納される。ここで、送信元コンピュータ情報は、通信元となるコンピュータを特定する情報であり、例えば、そのコンピュータのＩＰアドレスやユーザにより設定された名称情報が相当する。宛先コンピュータ情報は、通信先となるコンピュータを特定する情報であり、例えば、そのコンピュータのＩＰアドレスやユーザにより設定された名称情報が相当する。ユーザ情報は、ネットワーク上のコンピュータを使用して各種処理を実行するユーザを特定する情報であり、例えば、ネットワークにログインする際に入力するアカウント情報である。アクション対象情報は、ネットワーク上のアクションの対象を特定する情報である。例えば、クライアント１がサーバ２のＣドライブのＤｏｃｕｍｅｎｔ．ｔｅｘｔファイルを読み出した場合には、「サーバ２のＣドライブのＤｏｃｕｍｅｎｔ．ｔｅｘｔファイル」がアクション対象情報である。アクション情報は、Ｒｅａｄ（読み出し）、Ｗｒｉｔｅ（書き込み）、Ｄｅｌｅｔｅ（消去）、Ｐｒｉｎｔ（印刷）等の命令情報をいう。時刻情報は、アクションを実行した時刻を示す情報である。

【００４４】

表示装置３８は、液晶ディスプレイ、ＣＲＴ等の表示手段である。入力装置３９は、キーボード、マウス、マウスパッド等の入力手段である。

【００４５】

続いて、本発明にかかるネットワーク監視システムの処理フローについて、説明する。

【００４６】

図４のフローチャートに示されるように、ネットワーク監視コンピュータ３は、ネットワーク上を流れるパケットデータをデータ取得部３２によって取得する（Ｓ１０１）。特にこの例では、ネットワーク監視コンピュータ３は、リピータハブ５に接続されているため、クライアント１とサーバ２間で送受信される複数のパケットを取得する。取得されたパケットは、データ取得部３２によって取得データ記憶部３６に格納される。

【００４７】

次にネットワーク監視コンピュータ３は、データ解析部３３によって、Ｓ１０

１において取得された複数のパケットのデータ解析を実行する（Ｓ１０２）。このデータ解析においては、まず、各パケットの種類を特定する。そして、種類が特定されたパケットから一アクションを説明するために必要な情報（以下、アクション説明情報）を抽出する。当該アクション説明情報には、どのような種類の情報が含まれるかは、予めネットワーク監視プログラム上で定められている。この例におけるアクション説明情報は、送信元コンピュータ情報、宛先コンピュータ情報、ユーザ情報、アクション対象情報、アクション情報及びアクションの時刻情報が含まれる。このアクション説明情報は、解析データ記憶部３７に格納される。

【００４８】

続いて、表示情報生成部３４は、データ解析結果に基づいて表示情報を生成する（Ｓ１０３）。具体的には、データ解析部３３によって生成され、解析データ記憶部３７に格納されたアクション説明情報に基づき、予め指定された表示形式に従って、表示情報を生成する（Ｓ１０３）。表示形式については、後に詳述する。表示情報生成部３４によって生成された表示情報は、図示しない記憶領域に格納される。尚、表示情報生成部３４によって生成する表示情報には、少なくとも上述した解析データ記憶部３７に格納された送信元コンピュータ情報、宛先コンピュータ情報及びアクション情報を含ませ、これらを表示させることが望ましい。さらに、これらの情報に加えて、ユーザ情報、アクション対象情報及びアクションの時刻情報のいずれか又は全てを表示情報に含ませ、表示させることによって、さらに詳細にアクションの内容を把握することができる。

【００４９】

そして、ネットワーク監視コンピュータ３の入出力制御部３５は、表示情報生成部３４により生成され、所定記憶領域に格納された表示情報に基づき、表示装置３８によって表示を行う。表示画面例については、後に詳述する。

【００５０】

続いて、図５及び図６を用いて、簡略化した例に基づき、データの取得（Ｓ１０１）、データの解析（Ｓ１０２）及び表示情報の生成（Ｓ１０３）について説明する。まず、複数のパケットからなるデータを取得する（Ｓ１０１）。

【００５１】

そして、これらのデータの解析を行う（Ｓ１０２）。データ解析においては、まず、各パケットの種類の特定を行う。この例では、図５に示されるように、順に種類Ａ、種類Ｂ、種類Ｃ、種類Ｄ、種類Ｅ・・・であったものとする。ここで、パケットの種類Ａ乃至Ｅの内容について図６を用いて説明する。図６に示されるように、種類Ａは、接続パケットを示し、送信元コンピュータ情報及び宛先コンピュータ情報が含まれる。種類Ｂは、認証パケットを示し、ユーザ情報が含まれる。種類Ｃは、対象指定パケットを示し、アクション対象情報が含まれる。種類Ｄは、命令パケットを示し、アクション情報が含まれる。種類Ｅは、データパケットを示し、データが含まれる。

【００５２】

各パケットの種類の特定を実行した後にアクション説明情報を生成する。図５に示す例では、最初のパケットは、種類Ａのパケットであるから、その中に含まれる送信元コンピュータ情報、宛先コンピュータ情報を抽出する。次のパケットは、種類Ｂのパケットであるから、その中に含まれるユーザ情報を抽出する。さらに次のパケットは、種類Ｃのパケットであるから、その中に含まれるアクション対象情報を抽出する。同様にして、各パケットよりアクション説明情報を抽出する。そして、抽出されたアクション説明情報より、アクション毎にアクション説明情報を関連付ける。例えば、図５に示す例では、種類Ａ、Ｂ、Ｃ、Ｄのパケットを特定できれば一アクションのアクション説明情報を取得できるため、第１のアクションに相当するアクション説明情報は、１番目から４番目までのパケットによって得ることができる。第２のアクションに相当するアクション説明情報も図５に示される矢印によって関連付けられた複数のパケットより取得することができる。さらに第３のアクションに相当するアクション説明情報も図５に示される矢印によって関連付けられた複数のパケットより取得することができる。

【００５３】

そして、これらのアクション説明情報に基づいて、アクション毎の表示情報を生成する（Ｓ１０３）。

【００５４】

続いて、図７及び図８を用いて、本発明にかかるネットワーク監視コンピュータの画面表示例について説明する。図７は、テーブル形式により、ネットワーク上のアクションを表示させたものである。この画面表示例では、複数のアクション（この例では、８アクション）について、クライアント、アカウント、メッセージ、サーバーの情報からなるアクション説明情報がアクション毎にそれぞれ表示されている。この例では、ある所定時間内にネットワーク上で行われたアクションのアクション説明情報が表示されている。アクションが終了して一定時間経過後は、そのアクションのアクション説明情報は画面表示から消去される。

【００５５】

例えば、最上段に表示されたアクションについては、クライアントの情報として、クライアントのＯＳ（Ｏｐｅｒａｔｉｏｎ　Ｓｙｓｔｅｍ）を示す「２０００Ｐｒｏ」、クライアント名を示す「Ｈｅｍｐ」が表示されている。また、アカウントの情報として、アカウント名と関連付けられて予め設定されたアイコンと、アカウント名である「Ｋａｗａｓａｋｉ」が表示されている。そして、メッセージの情報として、アクション情報を示す「［ＮＧ］Ｃｒｅａｔｅ　Ｆｉｌｅ　Ｆａｉｌｕｒｅ」と、アクション対象情報を示す「¥新規作成文章．ｔｘｔ」が表示されている。さらに、サーバーの情報として、サーバーのＯＳを示す「２０００ＳＶＲ」と、サーバ名を示す「Ｆｉｌｅ　Ｓｅｒｖｅｒ」が表示されている。このような表示が行われることにより、ユーザは、最初のアクションが、「２０００Ｐｒｏ」のＯＳにより動作するクライアント「Ｈｅｍｐ」を用いて「Ｋａｗａｓａｋｉ」というユーザが「新規作成文章．ｔｘｔ」というファイルを「２０００ＳＶＲ」のＯＳにより動作するサーバー「Ｆｉｌｅ　Ｓｅｒｖｅｒ」に作成しようとして失敗したという内容を有するものであることを、極めて容易に把握することができる。

【００５６】

図８は、グラフ形式により、ネットワーク上のアクションを表示させたものである。図に示されるように、円が描かれ、その円の外側にクライアント及びサーバがそのＯＳとともに分散する形式で表示されている。そして、通信を行っているクライアントとサーバーが線により結ばれている。そして、この線に関連付け

られる形式でアクションの内容が表示されている。具体的には、アクションの内容の表記のうち、最初の文字がこの線上に重なるように表示することによって、線とアクションの内容を関連付けている。同じクライアント・サーバー間で通信が継続している間は、クライアントとサーバーを結ぶ線が表示されたままであり、新しいアクションが発生する度に、そのアクションの内容の表示が変わる。

【００５７】

次に、本発明にかかるネットワーク監視システムにおけるプレイバック機能について説明する。プレイバック機能とは、過去のネットワーク上のアクションを画面上で再生表示することをいう。具体的には、解析データ記憶部３７に記憶された解析データに基づいて、再生表示を実行する。この機能は、表示情報生成部２４によって実現される。当該ネットワーク監視システムにおいて、メニューよりプレイバック機能を選択し、表示項目を設定すると、図９に示されるような画面が表示される。この図では、再生表示している通信状態の時刻と、プレイバック機能の詳細を具体的にユーザにより指示するためのボタンを示す領域（ウィンドウ）が表示されている。図９に表示された例では、２００２年１０月８日１９時３６分３秒に表示されたアクションが実行されていることが判る。ボタンは、プレイバック機能を終了するボタン、一時停止するボタン、最初に戻すボタン、時間的に遡るボタン、再生ボタン、最後まで進めるボタン、拡大ボタンが含まれる。表示情報生成部２４は、画面上に表示されるボタンがユーザによりクリックされ、選択されたことを認識して、ボタンに応じた処理を実行する。

【００５８】

ここで、再生表示に関しては、実際のアクションが行われた時刻情報に従って、各アクションが実際のアクションと同じ時間間隔で表示されるよう再生表示することができる。この場合には、表示情報生成部２４は、解析データ記憶部３７に記憶された時刻情報に基づいて、実際のアクションと同じ時間間隔で表示されるよう制御する。また、ユーザの要求に応じて、略同じ時間間隔でアクションを連続的に再生表示させることも可能である。特に、速く表示させて、問題となるアクションを抽出する上では、有効な表示手段である。

【００５９】

図１０は、グラフ形式の表示画面において、プレイバック機能を実現するための領域を表示させたものである。その領域については、図９を用いて説明したものと同じであるため、説明を省略する。

【００６０】

さらに、本発明の実施の形態にかかるネットワーク監視システムでは、画面表示内容を設定することができる。図１１に設定画面表示例を示す。図に示されるように、設定画面では、アカウント、メッセージ、リソース、マシン名、ＯＳについて表示させる内容を選択することができる。また、表示情報に対する色やアイコンも選択することができ、これにより強調表示ができる。画面表示の設定は、通常の監視時のみならず、プレイバック機能を実現する際にも行うことができる。設定内容は、ネットワーク監視コンピュータ３上の図示しない記憶領域上に格納され、適宜表示情報生成部３４によって読み出される。

【００６１】

ここで、上述の例では、本発明にかかるネットワーク監視システムをクライアント・サーバシステムに適用した例について説明したが、これに限らず、ピア・ツー・ピアのシステムに適用することも可能である。

【００６２】

上述の例において、コンピュータのハードディスク、メモリ等の記憶手段等にインストールされた各種のプログラムは、様々な種類の記憶媒体に格納することが可能であり、また、通信媒体を介して伝達されることが可能である。ここで、記憶媒体には、例えば、フレキシブルディスク、ハードディスク、磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ、ＲＯＭカートリッジ、バッテリバックアップ付きＲＡＭメモリカートリッジ、フラッシュメモリカートリッジ、不揮発性ＲＡＭカートリッジ等を含む。また、通信媒体には、電話回線等の有線通信媒体、マイクロ波回線等の無線通信媒体等を含み、インターネットも含まれる。

【００６３】

【発明の効果】

本発明によれば、一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークを容易に監視することができるネットワーク

監視システム、ネットワーク監視方法及びネットワーク監視プログラムを提供することができる。

【図面の簡単な説明】

【図１】

本発明にかかるネットワーク監視システムが適用されるネットワークの構成を示す構成図である。

【図２】

本発明にかかるネットワーク監視コンピュータの構成を示すブロック図である。

【図３】

本発明にかかるネットワーク監視コンピュータの解析データ記憶部のデータ例を示す図である。

【図４】

本発明にかかるネットワーク監視システムの処理の流れを示すフローチャートである。

【図５】

本発明にかかるネットワーク監視システムの処理を説明するための説明図である。

【図６】

本発明にかかるネットワーク監視システムが適用されるネットワーク上を流れるパケットの種類の例を示す図である。

【図７】

本発明にかかるネットワーク監視システムによる画面表示例を示す図である。

【図８】

本発明にかかるネットワーク監視システムによる画面表示例を示す図である。

【図９】

本発明にかかるネットワーク監視システムにおいてプレイバック機能を実行した場合の画面表示例を示す図である。

【図１０】

本発明にかかるネットワーク監視システムにおいてプレイバック機能を実行した場合の画面表示例を示す図である。

【図１１】

本発明にかかるネットワーク監視システムにおいて表示内容を設定する画面表示例を示す図である。

【図１２】

パケットシーケンスの例を示す図である。

【符号の説明】

１　クライアント

２　サーバ

３　ネットワーク監視コンピュータ

４　ＬＡＮ

５　リピータハブ

３１　通信制御部

３２　データ取得部

３３　データ解析部

３４　表示情報生成部

３５　入出力制御部

３６　取得データ記憶部

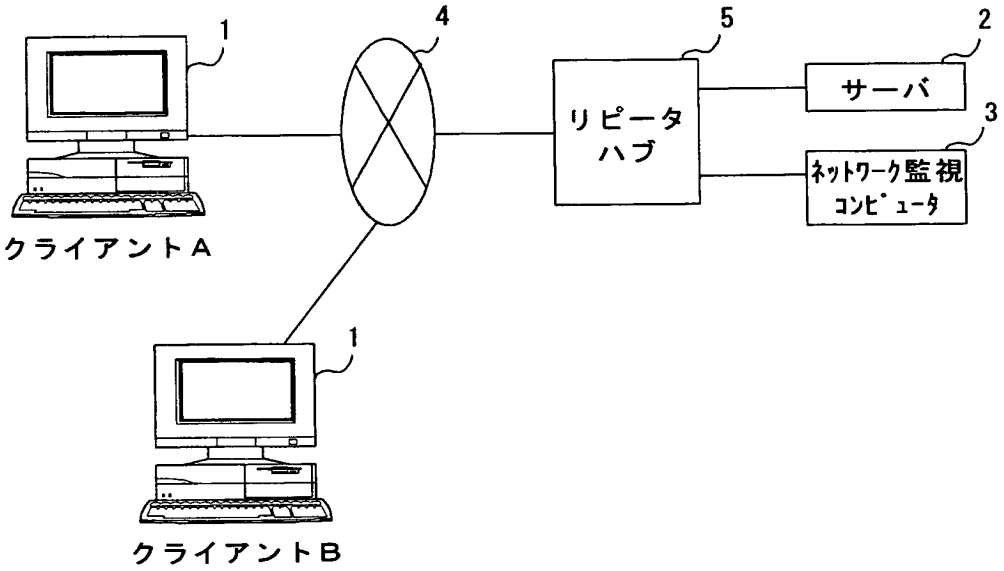
３７　解析データ記憶部

３８　表示装置

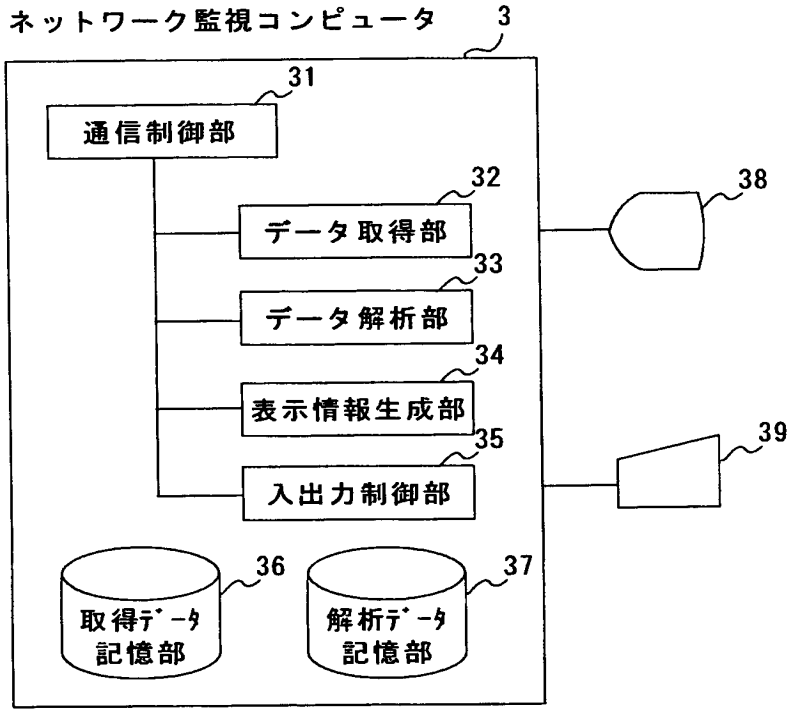
３９　入力装置

【書類名】　図面

【図１】


1
4
5
2
サーバ
3
リピータ
ハブ
ネットワーク監視
コンピュータ
クライアントＡ
1
クライアントＢ

【図２】

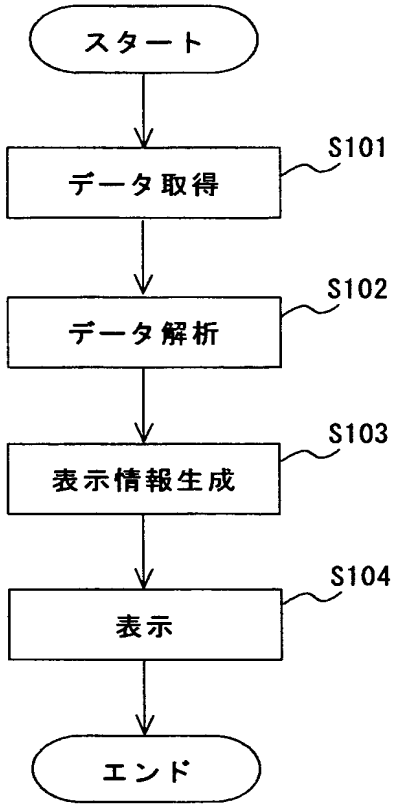

ネットワーク監視コンピュータ
3
31
通信制御部
32
データ取得部
38
33
データ解析部
34
表示情報生成部
39
35
入出力制御部
36
取得データ
記憶部
37
解析データ
記憶部

【図３】

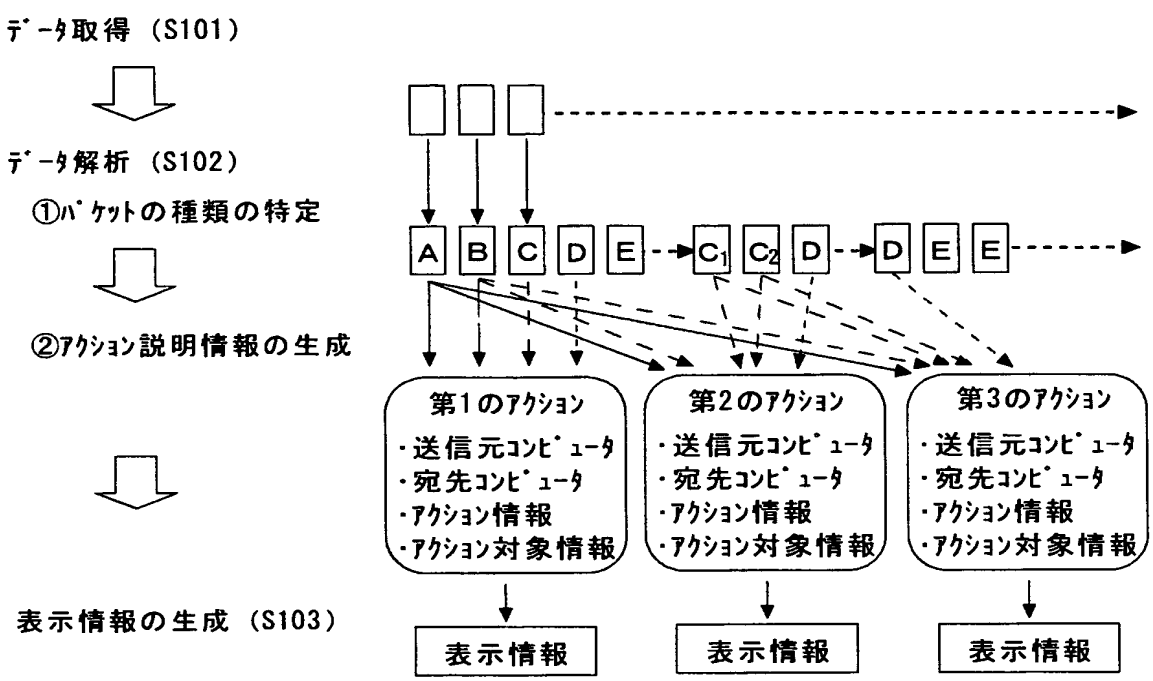
解析データ記憶部37

送信元ｺﾝﾋﾟｭｰﾀ情報	宛先ｺﾝﾋﾟｭｰﾀ情報	ﾕｰｻﾞ情報
ｱｸｼｮﾝ対象情報	ｱｸｼｮﾝ情報	時刻情報

【図４】



【図５】

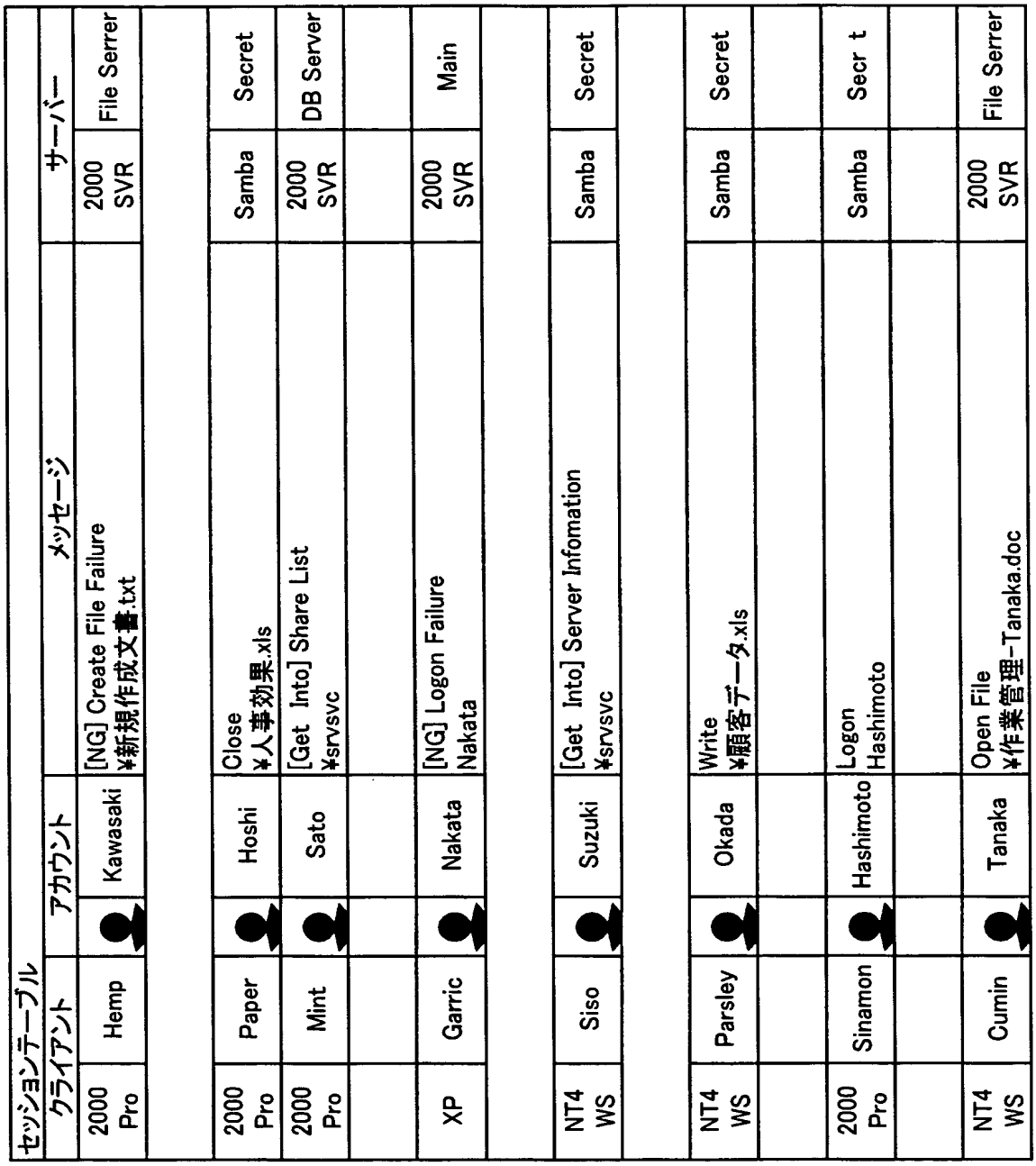


【図６】

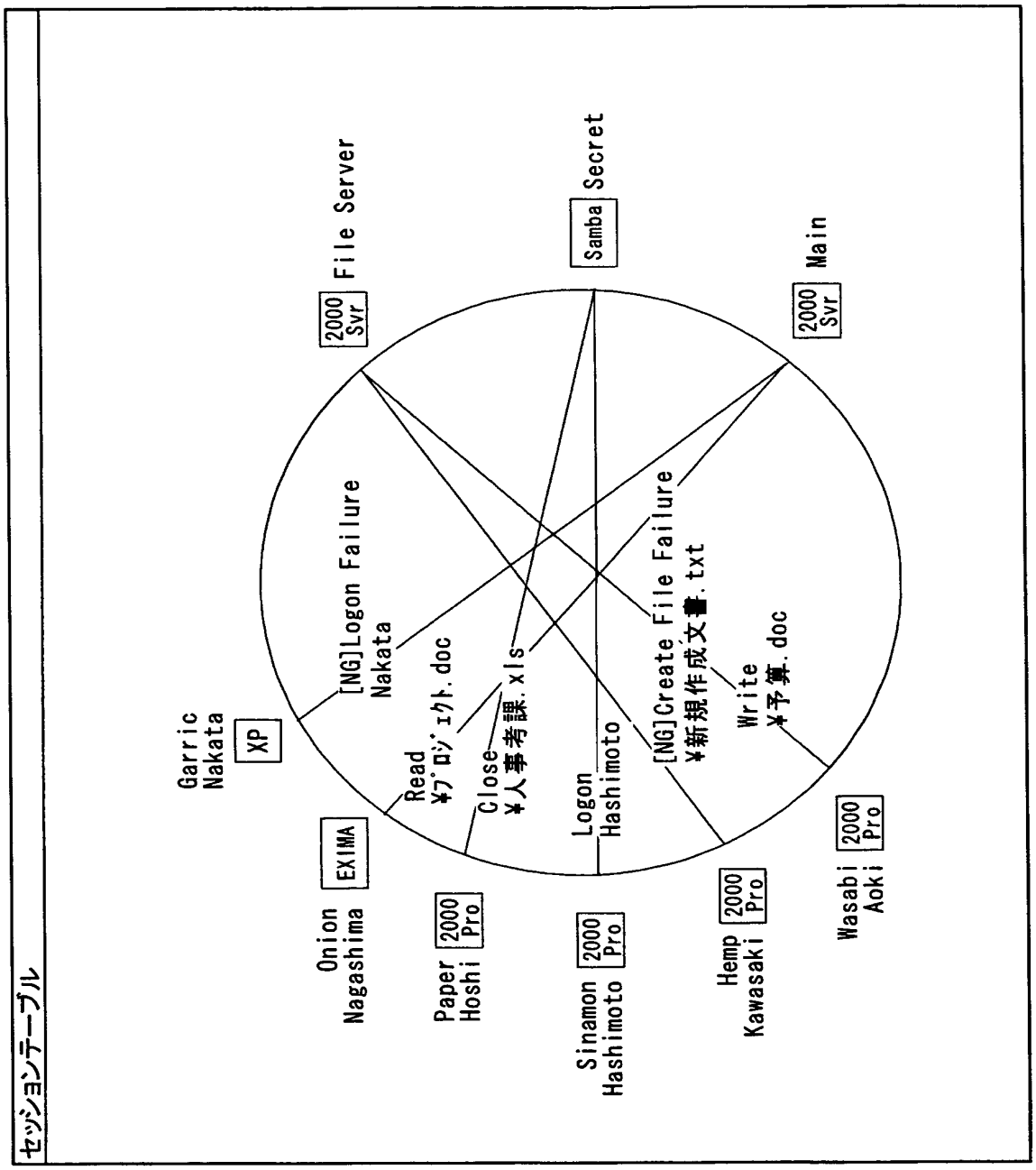
パケットの種類

種類	パケット名称	含まれる情報
A	接続パケット	送信元コンピュータ情報 宛先コンピュータ情報
B	認証パケット	ユーザ情報
C	対象指定パケット	アクション対象情報
D	命令パケット	アクション情報
E	データパケット	データ

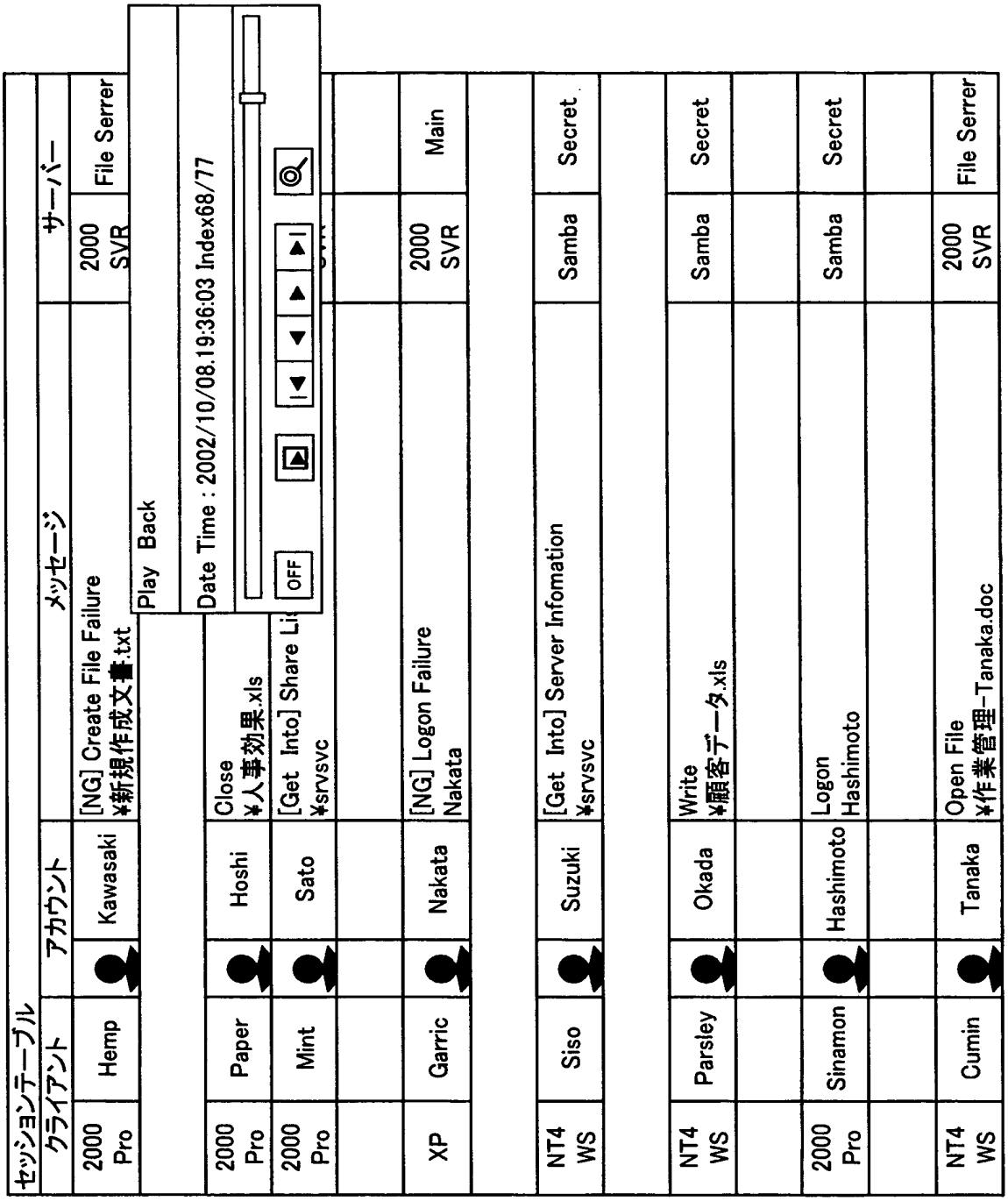
【図７】


セッションテーブル
クライアント
アカウント
メッセージ
サーバー
2000 Pro
Hemp
Kawasaki
[NG] Create File Failure ¥新規作成文書.txt
2000 SVR
File Serrer
2000 Pro
Paper
Hoshi
Close ¥人事効果.xls
Samba
Secret
2000 Pro
Mint
Sato
[Get Into] Share List ¥srvsvc
2000 SVR
DB Server
XP
Garric
Nakata
[NG] Logon Failure Nakata
2000 SVR
Main
NT4 WS
Siso
Suzuki
[Get Into] Server Infomation ¥srvsvc
Samba
Secret
NT4 WS
Parsley
Okada
Write ¥顧客データ.xls
Samba
Secret
2000 Pro
Sinamon
Hashimoto
Logon Hashimoto
Samba
Secr t
NT4 WS
Cumin
Tanaka
Open File ¥作業管理-Tanaka.doc
2000 SVR
File Serrer

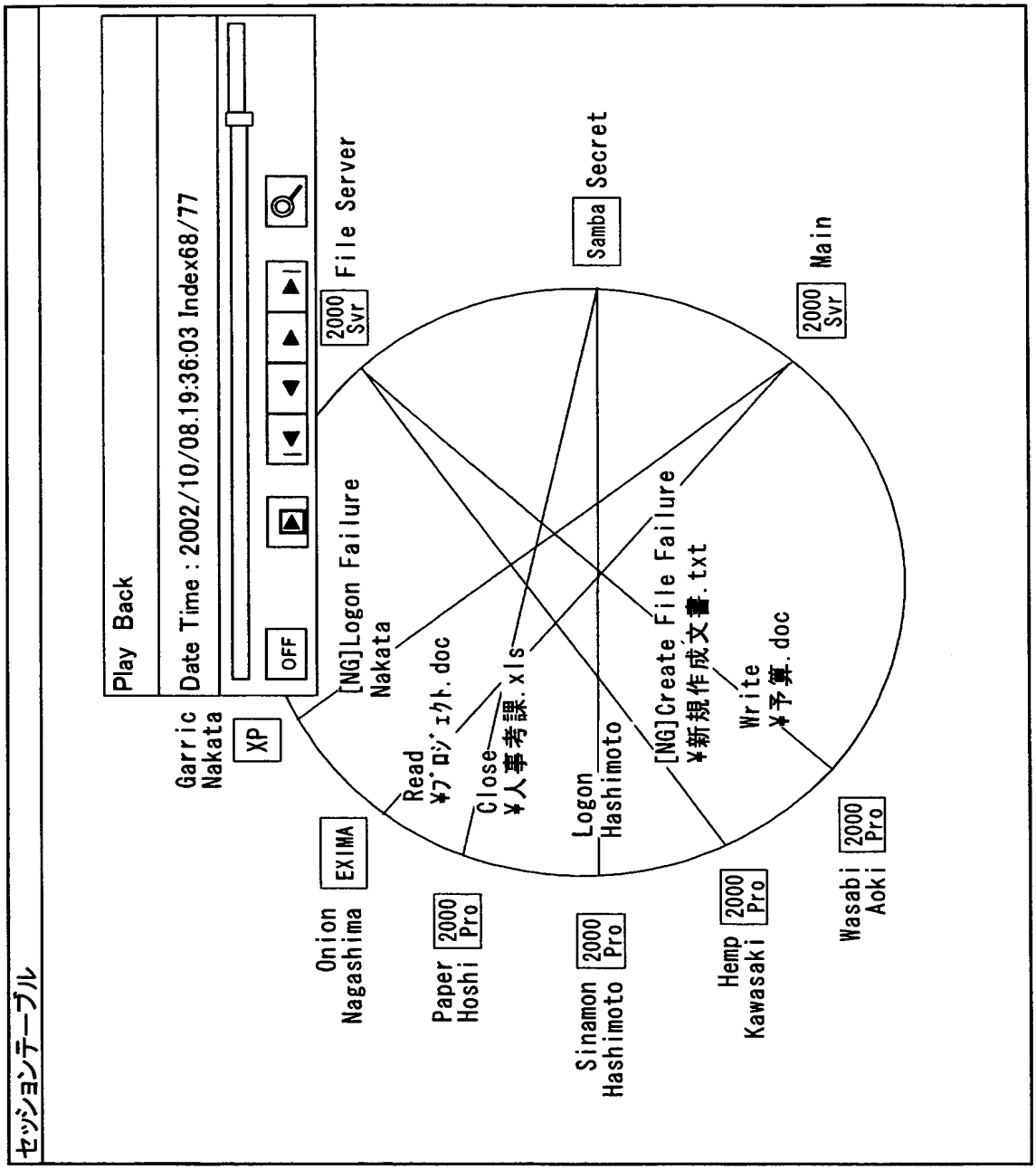
【図８】


セッションテーブル
Garric
Nakata
XP
Onion
Nagashima
EXIMA
Paper
Hoshi
2000 Pro
Sinamon
Hashimoto
2000 Pro
Hemp
Kawasaki
2000 Pro
Wasabi
Aoki
2000 Pro
2000 Svr
File Server
Samba
Secret
2000 Svr
Main
[NG]Logon Failure
Nakata
Read
¥ﾌﾟﾛｼﾞｪｸﾄ.doc
Close
¥人事考課.xls
Logon
Hashimoto
[NG]Create File Failure
¥新規作成文書.txt
Write
¥予算.doc

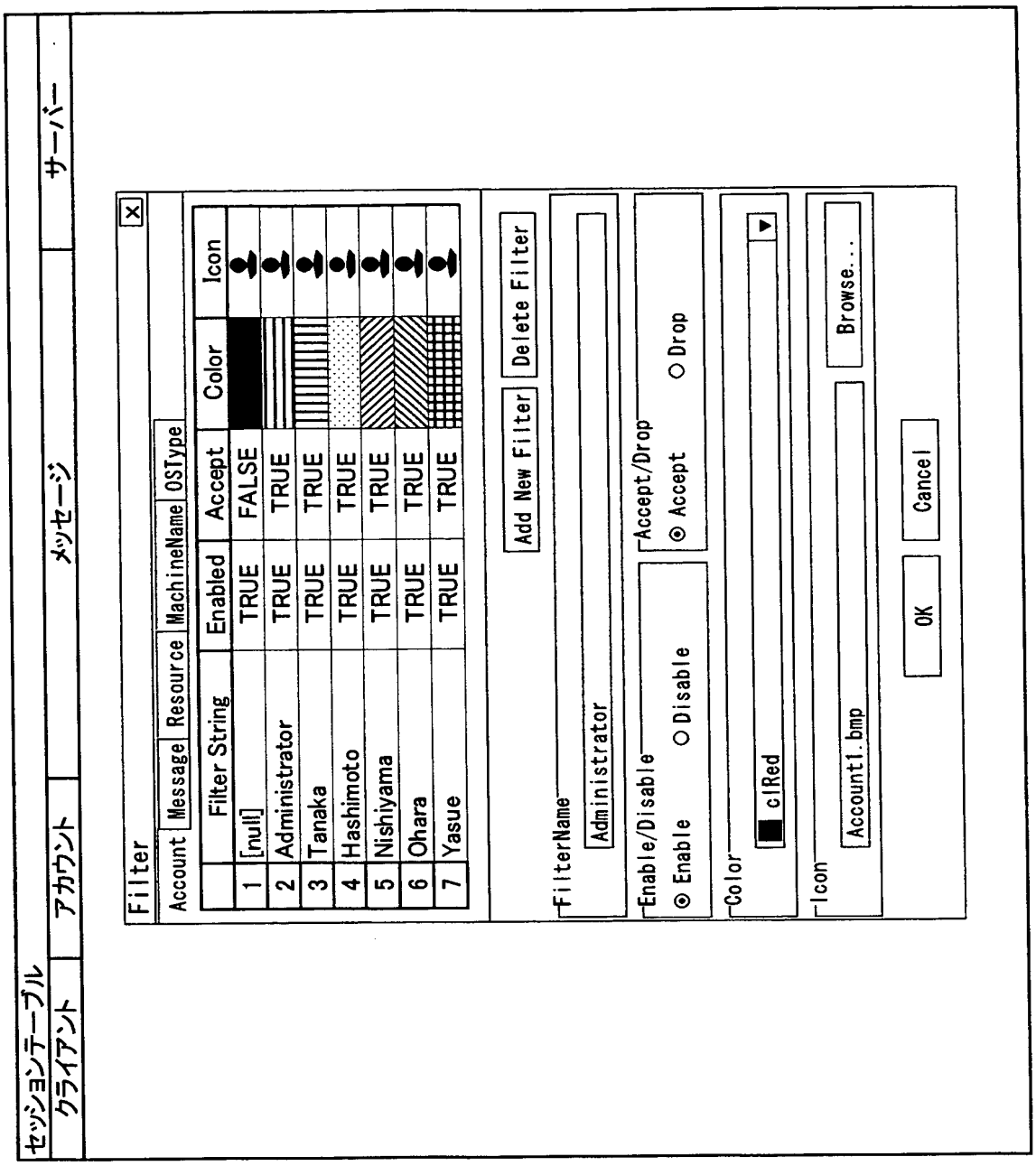
【図９】


セッションテーブル
クライアント
アカウント
メッセージ
サーバー
2000 Pro
Hemp
Kawasaki
[NG] Create File Failure ¥新規作成文書.txt
2000 SVR
File Serrer
Play Back
Date Time : 2002/10/08.19:36:03 Index68/77
OFF
2000 Pro
Paper
Hoshi
Close ¥人事効果.xls
2000 Pro
Mint
Sato
[Get Into] Share Li ¥srvsvc
XP
Garric
Nakata
[NG] Logon Failure Nakata
2000 SVR
Main
NT4 WS
Siso
Suzuki
[Get Into] Server Infomation ¥srvsvc
Samba
Secret
NT4 WS
Parsley
Okada
Write ¥顧客データ.xls
Samba
Secret
2000 Pro
Sinamon
Hashimoto
Logon Hashimoto
Samba
Secret
NT4 WS
Cumin
Tanaka
Open File ¥作業管理-Tanaka.doc
2000 SVR
File Serrer

【図１０】


セッションテーブル
Play Back
Date Time : 2002/10/08.19:36:03 Index68/77
OFF
Garric
Nakata
XP
2000 Svr
File Server
[NG]Logon Failure
Nakata
Samba
Secret
2000 Svr
Main
Read
¥ﾌﾟﾛｼﾞｪｸﾄ.doc
Close
¥人事考課.xls
Logon
Hashimoto
[NG]Create File Failure
¥新規作成文書.txt
Write
¥予算.doc
Onion
Nagashima
EXIMA
Paper
Hoshi
2000 Pro
Sinamon
Hashimoto
2000 Pro
Hemp
Kawasaki
2000 Pro
Wasabi
Aoki
2000 Pro

【図１１】


セッションテーブル
クライアント
アカウント
メッセージ
サーバー
Filter
Account
Message
Resource
MachineName
OSType
Filter String
Enabled
Accept
Color
Icon
1 [null] TRUE FALSE
2 Administrator TRUE TRUE
3 Tanaka TRUE TRUE
4 Hashimoto TRUE TRUE
5 Nishiyama TRUE TRUE
6 Ohara TRUE TRUE
7 Yasue TRUE TRUE
Add New Filter
Delete Filter
FilterName
Administrator
Enable/Disable
Enable
Disable
Accept/Drop
Accept
Drop
Color
clRed
Icon
Account1.bmp
Browse...
OK
Cancel

【図１２】

パケット番号	送信元 送信先	パケットの内容
1	C→S	セッション開始要求（パケットに送信元コンピュータ情報、宛先コンピュータ情報が含まれる）
2	S→C	セッション開始要求の応答
3	C→S	認証要求（1）（パケットにユーザ情報が含まれる）
4	S→C	認証要求（1） 認証情報の送信をクライアントへ要求
5	C→S	認証要求（2） 認証情報を送信
6	S→C	認証要求（2） 認証結果を返信
7	C→S	共有フォルダへの接続要求
8	S→C	共有フォルダへの接続応答
9～18	S↔C	共有フォルダのルートディレクトリの情報取得（ファイル一覧、各ファイルのファイル属性） 要求と応答の繰り返し
19	C→S	アクション対象ファイルのオープン要求（パケットに対象ファイル名が含まれる）
20	S→C	アクション対象ファイルのオープン要求の応答
21	C→S	ファイル保存領域情報の取得要求
22	S→C	ファイル保存領域情報の取得応答
23	C→S	ファイルへの書き込み要求（対象ファイルに対する書き込みを開始）
24～33	C→S	ファイルへ書き込むデータの転送
34	S→C	ファイルへの書き込み応答（対象ファイルに対する書き込み結果を返信）
35	C→S	ファイルのクローズ要求
36	S→C	ファイルのクローズ応答

【書類名】　　要約書

【要約】

【課題】

一アクションを説明するためのアクション説明情報が複数のパケットに分散されたネットワークを容易に監視することができるネットワーク監視システム、ネットワーク監視方法及びネットワーク監視プログラムを提供すること。

【解決手段】

本発明にかかるネットワーク監視システムでは、まず、データ取得部３２によって、ネットワーク上を流れる複数のパケットを取得する。そして、データ解析部３３は、データ取得部３２により取得された複数のパケットより、予め定められた一アクションを説明するためのアクション説明情報を取得する。そして、表示情報生成部３４は、このデータ解析部３３によって取得されたアクション説明情報に基づきネットワーク上の一アクションを一画面上で表示させる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－２９９９９７
受付番号	５０２０１５４５３６３
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１０月１６日

＜認定情報・付加情報＞

【提出日】　平成14年10月15日

次頁無

特願２００２－２９９９９７

出　願　人　履　歴　情　報

識別番号　　［０００００６６６６］

１．変更年月日　　１９９０年　８月２１日
［変更理由］　　新規登録
住　所　　東京都渋谷区渋谷２丁目１２番１９号
氏　名　　山武ハネウエル株式会社

２．変更年月日　　１９９８年　７月　１日
［変更理由］　　名称変更
住　所　　東京都渋谷区渋谷２丁目１２番１９号
氏　名　　株式会社山武